Issue Number : 5-5-2006-001515011

# 대한민국특허청
# KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

| | | |
|---|---|---|
| 출원번호 : Application Number | | 10-2003-0008512 |
| 출원년월일 : Date of Application | | 2003년 02월 11일<br>FEB 11, 2003 |
| 출원인 : Applicant(s) | | 엘지전자 주식회사<br>LG Electronics Inc. |

2006년 01월 10일

특허청
COMMISSIONER

◆ This certificate was issued by Korean Intellectual Property Office. Please confirm any forgery or alteration of the contents by an issue number or a barcode of the document below through the KIPOnet- Online Issue of the Certificates' menu of Korean Intellectual Property Office homepage (www.kipo.go.kr). But please notice that the confirmation by the issue number is available only for 90 days.

Issue Date : 2006.01.10

# 【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0002

【제출일자】 2003.02.11

【국제특허분류】 H04B

【발명의 국문명칭】 이동 통신 시스템에서 보안 설정 메시지를 처리하는 방법

【발명의 영문명칭】 Method of processing a security mode message in a mobile communication system

【출원인】

【명칭】 엘지전자 주식회사

【출원인코드】 1-2002-012840-3

【대리인】

【성명】 김용인

【대리인코드】 9-1998-000022-1

【포괄위임등록번호】 2002-027000-4

【대리인】

【성명】 심창섭

【대리인코드】 9-1998-000279-9

【포괄위임등록번호】 2002-027001-1

【발명자】

【성명의 국문표기】 천성덕

【성명의 영문표기】 CHUN,Sung Duck

【주민등록번호】 761223-1850520

【우편번호】 431-050

【주소】 경기도 안양시 동안구 비산동 샛별한양아파트 611동 1407호

【국적】 KR

【발명자】

【성명의 국문표기】 이승준

【성명의 영문표기】 YI,Seung June

【주민등록번호】 720625-1025312

【우편번호】 135-240

【주소】 서울특별시 강남구 개포동 대청아파트 303동 403호

【국적】 KR

【발명자】

【성명의 국문표기】 이영대

【성명의 영문표기】 LEE,Young Dae

【주민등록번호】 731215-1105411

【우편번호】 465-711

【주소】 경기도 하남시 창우동 신안아파트 419-1501

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다.

대리인 김용인 (인)

대리인 심창섭 (인)

【수수료】

【기본출원료】 20 면 29,000 원

【가산출원료】 8 면 8,000 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】 37,000 원

【첨부서류】 1.요약서·명세서(도면)_1통

# 【요약서】

## 【요약】

본 발명은 통신 시스템에 관한 것으로, 특히 제어 계층에서의 메시지를 처리하는 방법에 관한 것이다. 이 메시지를 처리하는 방법은 수신된 메시지가 보안 설정 제어 메시지인 경우, 이 제어 메시지에 근거하여 보안 관련 변수들을 재설정하고, 기설정된 보안 관련 변수들을 저장하는 단계, 상기 재설정된 변수들을 이용하여 상기 제어 메시지가 유효한 메시지인가를 체크하는 단계, 상기 제어 메시지가 유효하지 못한 경우, 상기 저장된 변수들을 복원하는 단계, 상기 복원된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 포함하여 이루어진다.

## 【대표도】

도 3

## 【색인어】

보안 검사, 무결성 검사, 보안 설정 제어 메시지

# 【명세서】

## 【발명의 명칭】

이동 통신 시스템에서 보안 설정 메시지를 처리하는 방법{Method of processing a security mode message in a mobile communication system}

## 【도면의 간단한 설명】

<1> 도 1은 일반적인 UMTS의 망 구조를 나타낸 도면이다.

<2> 도 2는 3GPP 무선 접속망 규격을 기반으로 한 단말기와 UTRAN사이의 무선 인터페이스 (Radio Interface) 프로토콜의 구조를 나타낸 다이어그램이다.

<3> 도 3은 본 발명의 바람직한 실시예에 따른 보안 설정 제어 메시지의 처리 방법을 나타낸 플로우 챠트이다.

<4> 도 4는 본 발명의 바람직한 실시예에 따른 보안 관련 환경 변수들 중 COUNT-I의 구성을 도시한 것이다.

<5> 도 5는 본 발명의 바람직한 실시예에 따른 무결성 검사의 인증값 생성 알고리즘의 일 예를 도시한 것이다.

## 【발명의 상세한 설명】

### 【발명의 목적】

### 【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 통신 시스템에 관한 것으로, 특히 이동 통신 시스템에서 보안 설정 메시지를 처리하는 방법에 관한 것이다.

<7> UMTS (Universal Mobile Telecommunications System)는 유럽식 표준인 GSM(Global System for Mobile Communications) 시스템으로부터 진화한 제3 세대 이동 통신 시스템으로, GSM 핵심망(Core Network)과 WCDMA (Wideband Code Division Multiple Access) 접속기술을 기반으로 하여 보다 향상된 이동통신서비스의 제공을 목표로 한다.

<8> UMTS의 표준화 작업을 위해, 1998년 12월에 유럽의 ETSI, 일본의 ARIB/TTC, 미국의 T1 및 한국의 TTA 등은 제3세대 공동프로젝트(Third Generation Partnership Project ; 이하, 3GPP라 약칭함)라는 프로젝트를 구성하였고, 현재까지 UMTS의 세부적인 표준명세서(Specification)를 작성 중에 있다.

<9> 3GPP에서는 UMTS의 신속하고 효율적인 기술을 개발하기 위해, 망 구성 요소들과 이요소들의 동작에 대한 독립성을 고려하여 UMTS의 표준화 작업을 5개의 기술규격그룹(Technical Specification Groups; 이하, TSG라 약칭함)으로 나누어 진행하고 있다.

<10> 각 TSG는 관련된 영역내에서 표준규격의 개발, 승인, 그리고 그 관리를 담당하는데, 이들 중에서 무선 접속망 (Radio Access Network : 이하 RAN이라 약칭함) 그룹(TSG RAN)은 UMTS에서 WCDMA 접속 기술을 지원하기 위한 새로운 무선접속망인 UMTS 무선망 (Universal Mobile Telecommunications Network Terrestrial Radio Access Network;이하, UTRAN이라 약칭함)의 기능, 요구사항 및 인터페이스에 대한 규격을 개발한다.

<11> 도 1은 일반적인 UMTS의 망 구조를 나타낸 도면이다.

<12> 도 1을 참조하면, UMTS 시스템은 단말기(100)와 UTRAN(200) 및 핵심망(300)으로 구성된다.

<13> 상기 UTRAN(200)은 다수의 무선 망 서브시스템(Radio Network Sub-systems)(10a~10n)으로 구성된다. 각 무선 망 서브시스템(10a, 10b, ..., 10n)은 하나의 무선 망 제어기(Radio Network Controller;이하 RNC라 약칭함)(12;14)와, 상기 RNC(12;14)에 의해서 관리되는 다수의 Node B들(11a~11b;13a~13b)로 구성된다. 상기 Node B들(11a~11b;13a~13b)은 상기 RNC(12;14)에 의해서 관리된다. 상기 Node B들(11a~11b;13a~13b)은 물리 계층 레벨에서 상기 단말기(100)로부터 전송되는 상향 링크 신호들을 수신하고, 상기 단말기(100)로 하향 링크 신호들을 송신한다. 다시 말하면, 상기 Node B들(11a~11b;13a~13b)은 상기 단말기(100)로/로부터의 신호들을 송/수신하는 역할을 수행함으로써, 상기 단말기(100)를 상기 UTRAN(200)으로 접속시키기 위한 접속점(Access Point) 역할을 한다. 상기 RNC(12;14)는 무선 자원의 할당 및 관리를 담당하고, 상기 Node B들(11a~11b;13a~13b)을 상기 핵심망(300)으로 접속시키기 위한 접속점 역할을 한다. 상기 UMTS 망과 접속한 각 단말기는 UTRAN(200) 내의 특정한 RNC(12;14)에 의해서 관리되고 있는데, 이 RNC를 SRNC(Serving RNC)라고 하고, 상기 SRNC는 특정 단말기의 데이터 전송을 위해 상기 핵심망(300)과의 접속점 역할을 하며, 서비스의 제공에 알맞은 무선 자원을 상기 특정 단말기에게 할당한다. 상기 UTRAN(200)을 통해 상기 핵심망(300)과 접속한 단말기는 오직 하나의 SRNC만을 갖는다. 일반적으로, 단말기(100)와 핵심망(300) 사이의 접속을 위해 하나의 RNC가 이용되지만, 상기 단

말기(100)의 이동에 의해 다른 RNC가 담당하는 영역으로 이동하는 경우에는 상기 단말기(100)가 이동한 지역의 RNC를 경유하여 상기 SRNC와 연결된다. 이와 같이, SRNC를 제외하고 단말기가 경유하게 되는 모든 RNC들을 DRNC(Drift RNC)들이라 부르며, 상기 DRNC들은 단순히 사용자 데이터를 라우팅하거나 공용 자원인 코드를 할당하는 부분적인 기능만을 수행한다. 단말기의 관점에서 SRNC와 DRNC의 구분은 논리적인 구분이다. 반면, UTRAN(200)에서의 RNC(12;14)와, Node B들 (11a~11b;13a~13b)의 종속적인 관계에 따라, Node B들(11a~11b;13a~13b)의 관점에서, 특정 Node B의 관리를 담당하는 RNC를 CRNC라 부르고, 상기 CRNC는 자신이 관리하고 있는 셀 내에서의 트래픽 부하 제어와, 폭주 제어 및 이들 셀 내에 설정되는 새로운 무선 링크에 대한 수락 제어 기능을 수행한다. 상기 UTRAN(200)의 구조상 각 Node B(11a~11b;13a~13b)는 반드시 하나의 CRNC만을 갖는다.

<14> 상기 UTRAN(200)은 상기 단말기(100)와 상기 핵심망(300) 사이의 통신을 위해 무선접속 운반자(Radio Access Bearer; 이하 RAB이라 약칭함)를 구성하고, 유지하고, 관리한다. 상기 핵심망(300)은 종단간(end-to-end)의 서비스 품질(Quality of Service; 이하 QoS라 약칭함) 요구 사항을 상기 RAB에 적용하고, 상기 RAB은 상기 핵심망(300)이 설정한 QoS 요구 사항을 지원한다. 따라서, 상기 UTRAN(200)은 상기 RAB을 구성하고, 유지하고, 관리함으로써 종단간의 QoS 요구사항을 충족시킬 수 있다.

<15> 상기 RAB 서비스는 다시 하위 개념의 Iu 운반자 서비스(Iu Bearer Service)와 무선 운반자 서비스(Radio Bearer Service)로 구분된다. 상기 Iu 운반자 서비스

는 상기 UTRAN(200)과, 상기 핵심망(300) 경계 노드 사이에서 사용자 데이터의 신뢰성 있는 전송을 수행한다. 상기 무선 운반자 서비스는 상기 단말기(100)와, 상기 UTRAN(200) 사이에서 사용자 데이터의 신뢰성 있는 전송을 수행한다.

<16> 한편, 특정 단말에게 제공되는 서비스는 회선 교환 서비스와 패킷 교환 서비스로 구분될 수 있다. 예를 들어, 일반적인 음성 전화 서비스는 상기 회선 교환 서비스에 속하고, 인터넷접속을 통한 웹브라우징서비스는 상기 패킷 교환 서비스로 분류된다. 상기 회선 교환 서비스를 지원하는 통신 시스템에서 RNC(12;14)는 상기 핵심망(300)의 교환기(Mobile Switching Center;이하 MSC)(20)와 연결되고, 상기 MSC(20)는 외부 망으로부터 요청되거나, 상기 외부 망으로 요청되는 음성(voice) 타입의 호(call)의 접속을 관리하는 GMSC(Gateway Mobile Switching Center)(30)와 연결된다. 상기 패킷 교환 서비스를 지원하는 통신 시스템에서, 상기 RNC(12;14)는 상기 핵심망(300)의 SGSN(Serving GPRS(General Packet Radio Service) Support Node;이하 SGSN)(40)과, GGSN(Gateway GPRS Support Node; 이하 GGSN)(50)과 연결된다. 상기 GGSN(50)은 인터넷 또는 외부 패킷 네트워크와의 연동을 위한 게이트웨이의 기능을 수행한다. 상기 SGSN(40)은 상기 GGSN(20)에 연결되어 이동 단말기의 이동성을 관리하고, 패킷 교환기 기능을 수행한다.

<17> 다른 한편, 다수의 망 구성 요소들 사이에는 서로간의 통신을 위해 정보를 주고 받을 수 있는 인터페이스(Interface)가 있다. 상기 RNC(12;14)와 상기 핵심망(300)과의 인터페이스를 Iu 인터페이스라고 정의한다. 상기 Iu 인터페이스가 패킷 교환 영역의 구성 요소와 연결되는 곳에서는 Iu-PS라고 하고, 상기 Iu 인터페이스

가 회선 교환 영역의 구성 요소와 연결된 곳에서는 Iu-CS라고 정의한다.

<18> 도 2는 3GPP 무선 접속망 규격을 기반으로 한 단말기와 UTRAN사이의 무선 인터페이스 (Radio Interface) 프로토콜의 구조를 나타낸 다이어그램이다.

<19> 도 2를 참조하면, 상기 무선 인터페이스 프로토콜은 수평적으로 물리계층(PHY), 데이터 링크 계층 및 네트워크 계층으로 이루어진다. 상기 무선 인터페이스 프로토콜은 수직적으로는 데이터 정보를 제공하기 위한 사용자 평면(User Plane)과, 제어신호(Signaling)를 제공하기 위한 제어 평면(Control Plane)으로 구분된다. 상기 사용자 평면은 음성이나 IP(Internet Protocol;이하 IP) 패킷의 전송 등과 같이 사용자의 트래픽 정보를 제공하기 위한 영역이다. 상기 제어 평면은 망의 인터페이스나 호의 유지 및 관리 등을 위한 제어정보를 제공하기 위한 영역이다.

<20> 도 2의 프로토콜 계층들은 통신시스템에서 널리 알려진 개방형 시스템간 상호접속 (Open System Interconnection; OSI) 기준 모델의 하위 3개 계층을 바탕으로 L1 (제1계층), L2 (제2계층), L3(제3계층)로 구분된다.

<21> 상기 L1 계층은 다양한 무선 전송 기술을 이용해 상위 계층에 정보 전송 서비스(Information Transfer Service)를 제공한다. 상기 L1 계층은 상위 계층의 매체 접속 제어(Medium Access Control;이하 MAC) 계층과 전송 채널(Transport Channel)을 통해 연결된다. 상기 전송채널을 통해 상기 MAC 계층과 상기 물리 계층 사이에서 데이터가 전달된다.

<22> 상기 MAC 계층은 무선 자원의 할당 및 재할당을 위한 MAC 파라미터의 재할당

서비스를 제공한다. 상기 MAC 계층은 상위 계층의 무선 링크 제어(Radio Link Control;이하 RLC) 계층과는 논리 채널(Logical Channel)을 통해 연결된다. 상기 MAC 계층과 상기 RLC 계층 사이에서 전달되는 데이터 정보의 종류에 따라 여러 타입들의 논리 채널들이 있다..

<23> 상기 제어 평면의 정보를 전송할 경우에는 제어 채널(Control Channel)을 이용하고, 상기 사용자 평면의 정보를 전송하는 경우는 트래픽 채널(Traffic Channel)을 사용한다.

<24> 상기 MAC 계층은 관리하는 전송 채널의 종류에 따라 MAC-b 부계층(Sublayer), MAC-d 부계층, MAC-c/sh 부계층으로 구분된다. 상기 MAC-b 부계층은 시스템 정보(System Information)의 방송을 담당하는 전송 채널인 방송 채널(Broadcast Channel;이하 BCH)를 관리한다. 상기 MAC-c/sh 부계층은 다른 단말기들과 공유되는 순방향 접속 채널(Forward Access Channel; 이하 FACH)이나 하향링크 공유 채널 (Downlink Shared Channel;이하 DSCH) 등의 공통 전송 채널을 관리한다. UTRAN에서 CRNC(Controlling RNC)가 상기 MAC-c/sh 부계층을 포함한다. 상기 MAC-c/sh 계층은 셀 내의 모든 단말기들이 공유하는 채널들을 관리하므로, 각 셀에 대해서 하나씩 존재한다. 각 단말기는 하나의 MAC-c/sh 부계층을 포함한다. 상기 MAC-d 부계층은 특정 단말기에 대한 전용 전송 채널인 전용 채널(Dedicated Channel;이하 DCH)를 관리한다. SRNC(Serving Radio Network Controller)가 상기 UTRAN의 MAC-d 부계층을 포함한다. 각 단말기도 하나씩의 MAC-d 부계층을 포함한다.

<25> 상기 RLC 계층은 신뢰성 있는 데이터의 전송을 지원하며, 상위 계층으로부터 전달된 RLC 서비스 데이터 단위(Service Data Unit; 이하, SDU라 약칭함)들을 분할 및 연결 (Segmentation and Concatenation)한다. 상기 상위 계층로부터 전달된 RLC SDU는 상기 RLC 계층에서 처리할 수 있는 RLC 데이터 단위들로 나누어지고, 이 나누어진 RLC 데이터 단위들에 헤더(Header) 정보가 부가되어 프로토콜 데이터 단위(Protocol Data Unit; 이하, PDU라 약칭함)의 형태로 상기 MAC 계층에 전달된다. 상기 RLC 계층은 상위 계층으로부터 전달된 RLC SDU 또는 RLC PDU들을 저장하기 위한 RLC 버퍼를 포함한다.

<26> 패킷 데이터 수렴 프로토콜(Packet Data Convergence Protocol; 이하 PDCP라 약칭함) 계층은 RLC 계층의 상위에 위치한다. 상기 PDCP 계층은 IPv4나 IPv6와 같은 네트워크 프로토콜을 통해 전송되는 데이터가 상대적으로 대역폭이 작은 무선 인터페이스상에서 효율적으로 전송될 수 있도록 한다. 이를 위해, 상기 PDCP 계층은 유선망에서 사용되는 불필요한 제어정보를 줄여주는 기능을 수행하는데, 이 기능을 헤더압축(Header Compression)이라 부르며, IETF(Internet Engineering Task Force)라는 인터넷 표준화 그룹에서 정의하는 헤더압축기법인 RFC2507과 RFC3095(Robust Header Compression: ROHC)를 사용할 수 있다. 이들 방법은 데이터의 헤더(Header) 부분에서 반드시 필요한 정보만을 전송하도록 하여, 보다 적은 제어정보를 전송하므로 전송될 데이터량을 줄일 수 있다.

<27> 방송/멀티캐스트제어(Broadcast/Multicast Control; 이하 BMC라 약칭함) 계층은 상기 핵심망으로부터 전달된 셀 방송 메시지(Cell Broadcast Message; 이하

CB 메시지라 약칭함 )를 전송할 UE(User Equipment, 예를 들어, 단말기)들을 스케줄링하고, 상기 스케줄링 결과에 근거하여 특정 셀(들)에 위치한 해당 UE들에게 상기 셀 방송 메시지를 전달한다. 상기 UTRAN에서 상위 계층으로부터 전달된 CB 메시지는 메시지 ID, 일련 번호(Serial Number) , 코딩 정보(coding scheme) 등의 헤더 정보가 더해져 BMC 메시지로 생성된다. 그리고, 이 BMC 메시지는 RLC 계층에 전달된다. 상기 RLC 계층은 상기 BMC 메시지에 RLC 헤더 정보를 부가하여, 논리 채널 CTCH (Common Traffic Channel)를 통해 MAC 계층에 전달한다. 상기 논리채널 CTCH 는 전송채널 FACH (Forward Access Channel)와 물리채널 S-CCPCH (Secondary Common Control Physical Channel)에 매핑된다.

<28> L3의 가장 하부에 위치한 무선자원제어(Radio Resource Control; 이하 RRC라 약칭함) 계층은 제어 평면에서만 정의된다. 무선 운반자 (Radio Bearer; 이하 RB라 약칭함)들의 설정, 재설정 및 해제와 관련되어 전송 채널 및 물리채널들의 제어를 담당한다. 이때, RB는 UE와 UTRAN간의 데이터 전달을 위해 제2계층에 의해 제공되는 서비스를 의미한다. 상기 RB가 설정된다는 것은 특정 서비스를 제공하기 위해 필요한 프로토콜 계층 및 채널의 특성을 규정하고, 각각의 구체적인 파라미터 및 동작 방법을 설정하는 과정을 의미한다.

<29> 참고로, RLC 계층은 상위에 연결된 계층에 따라 사용자 평면에 속할 수도 있고 제어 평면에 속할 수도 있다. 상기 제어평면에 속하는 경우에는 무선 자원 제어 (Radio Resource Control; 이하 RRC라 약칭함) 계층으로부터 데이터를 전달 받는 경우에 해당되고, 그 외의 경우는 사용자 평면에 해당한다.

<30> 또한, 상기 도 2에서 알 수 있듯이 RLC 계층과 PDCP 계층의 경우에는, 하나의 계층 내에 여러개의 엔터티(Entity)들이 존재할 수 있다. 이는 하나의 단말기가 여러 개의 무선 운반자들을 갖고, 각 무선 운반자에 대하여 일반적으로 오직 하나의 RLC 엔터티 및 PDCP 엔터티가 사용되기 때문이다.

<31> 한편, 단말기와 UTRAN 사이에는 데이터를 주고받기 위한 채널들이 정의되어 사용된다. 상기 단말기와 상기 UTRAN의 물리계층은 물리채널(Physical Channel)을 이용해 데이터를 주고 받는다. 이와 함께, UMTS의 무선접속 구간에서는 물리채널 이외에 프로토콜 계층간의 데이터 전송 통로를 전송채널(Transport Channel)과 논리채널(Logical Channel)이라고 정의해서 사용한다. 상기 논리 채널은 RLC 계층과 MAC 계층 사이에서, 상기 전송 채널은 MAC 계층과 물리 계층 사이에서 데이터의 교환을 위해 제공되는 채널로서, 상기 MAC 계층에서는 전송채널 간의 매핑이, 물리채널에서는 전송채널과 물리채널 간의 매핑이 이루어진다.

<32> 한편, 단말기와 UTRAN 사이에는 데이터를 주고받기 위한 채널들이 정의되어 사용된다. 이에 대해 좀 더 자세히 살펴보도록 하자.

<33> 단말기와 UTRAN의 물리계층은 물리채널(Physical Channel)을 이용해 데이터를 주고 받는다. 이와 함께, UMTS의 무선접속 구간에서는 물리채널 이외에 프로토콜 계층간의 데이터 전송통로를 전송채널(Transport Channel)과 논리채널(Logical Channel)이라고 정의해서 사용한다. 논리채널은 RLC계층과 MAC계층 사이에서, 전송채널은 MAC계층과 물리계층 사이에서 데이터의 교환을 위해 제공되는 채널이다. MAC계층에서는 전송채널 간의 매핑이, 물리채널에서는 전송채널과 물리채널 간의

매핑이 이루어진다.

<34> 단말기와 UTRAN은 다양한 메시지를 주고받는다. 이 메시지들은 포함된 데이터를 보호하기 위해서 대부분의 경우 보안검사(Security Check)를 수행한다. 이런 보안 검사에는 암호화(Ciphering)와, 무결성 검사가(Integrity Check) 있다. 상기 암호화는 전송하는 측과 수신하는 측이 둘만 알고 있는 특정한 마스크(MASK)를 메시지에 더하여, 이 마스크를 알지 못하는 제3자가 메시지의 내용을 알지 못하게 하는 것이 목적이다. 그런데, 무결성 검사는 상기 암호화와는 달리 전송되어진 메시지가 중간에 내용이 바뀌지 않았는지를 확인하거나, 인증되지 않은 곳으로부터 온 것인지 아닌지를 확인하기 위해서 사용된다. 즉, 상기 무결성 검사는 수신된 메시지의 내용이 제3자에 의해 중간에서 의도적으로 변경되었는지 아닌지를 체크하기 위해서 필요한 과정이다. 현재 UMTS에서는 대부분의 RRC 계층으로 전달되는 메시지와 RRC의 상위 계층으로 전송되는 대부분의 제어 메시지에 대해서 암호화와 무결성 검사를 동시에 수행하게 된다. 그 외의 일반 사용자 데이터는 암호화만 수행하게 된다. 이런 무결성 검사는 RRC 계층에서 수행된다.

<35> 이와 같이, 송신측과 수신측의 중간에서 제 3자에 의해 변경된 내용을 포함하는 메시지 또는 인증되지 않는 송신측으로부터 온 메시지를 걸러내기 위해서 상기 수신측은 상기 수신된 메시지에 대해서 무결성 검사를 하고, 상기 수신된 메시지가 이 무결성 검사를 통과하는지에 따라 상기 수신된 메시지의 폐기 여부를 결정한다.

<36> 상기 수신된 메시지 중의 일 예로 보안 설정 제어 메시지가 있을 수 있다.

상기 보안 설정 제어 메시지는 단말기와 네트워크(예를 들어, UTRAN) 사이의 연결에서 추후에 전송되는 데이터에 대한 보안화를 시작하려고 하거나, 기존에 보안화가 이루어지고 있던 연결에서 사용되는 보안관련 환경 변수값들을 제어할 때 사용되는 메시지이다. 상기 보안 설정 제어 메시지에 포함된 내용 중 보안관련 환경 변수값들을 제어하는 것과 관련된 정보를 보안관련 환경설정정보라 한다.

<37> 상기 수신측은 상기 보안 설정 제어 메시지를 수신하고, 이 보안 설정 제어 메시지에 포함된 정보를 이용하여, 자신의 보안관련 환경 변수를 갱신한다. 상기 수신측은 상기 갱신된 보안 관련 환경변수를 이용하여 상기 보안 설정 제어 메시지 자체에 대한 무결성 검사를 수행한다. 상기 보안 설정 제어 메시지도 인증되지 않은 송신측으로부터 전송될 수 있고, 송신측과 수신측 사이에서 메시지의 내용이 제3자에 의해서 변경되었을 수도 있으므로, 상기 수신된 보안 설정 제어 메시지가 무결성 검사를 통과하지 못할 수가 있다. 따라서, 이 경우도 메시지가 잘못된 것으로 판단하고, 수신된 보안 설정 제어 메시지를 즉시 폐기해야 하며, 이 보안 설정 제어 메시지에 포함된 보안 관련 환경설정 정보도 신뢰할 수 없으므로, 사용해서는 안 된다. 그런데, 수신측은 이 보안 설정 제어 메시지를 수신하면, 기설정된 보안 관련 환경 변수를 이 메시지에 포함된 보안 관련 환경 설정 정보로 갱신하고, 기존의 보안관련 환경변수는 폐기하였다. 따라서, 수신측이 가진 보안관련 환경변수와 송신측이 가진 보안관련 환경변수는 더 이상 일치하지 않게 되고, 추후의 메시지 교환은 불가능하게 되고, 수신측은 더 이상 원하는 서비스를 더 이상 제공받을 수 없는 문제점이 발생하게 된다.

【발명이 이루고자 하는 기술적 과제】

<38> 이상에서 언급한 종래 기술의 문제점을 감안하여 안출한 것으로서, 본 발명의 목적은 이동 통신 시스템에서 보안 설정 메시지를 처리하는 방법을 제공하기 위한 것이다.

<39> 본 발명의 다른 목적은 송/수신측간에 보안 설정 환경 변수들이 일치하도록 하는 이동 통신 시스템에서 보안 설정 메시지를 처리하는 방법을 제공하기 위한 것이다.

<40> 이상과 같은 본 발명의 일 특징에 따르면, 메시지를 처리하는 방법은 수신된 메시지가 보안 설정 제어 메시지인 경우, 이 제어 메시지에 근거하여 보안 관련 변수들을 재설정하고, 기설정된 보안 관련 변수들을 저장하는 단계, 상기 재설정된 변수들을 이용하여 상기 제어 메시지가 유효한 메시지인가를 체크하는 단계, 상기 제어 메시지가 유효하지 못한 경우, 상기 저장된 변수들을 복원하는 단계, 상기 복원된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 포함하여 이루어진다.

<41> 본 발명의 다른 특징에 따르면, 무선 자원 제어 계층에서의 메시지를 처리하는 방법은 수신된 메시지가 보안 설정 제어 메시지인 경우, 이 제어 메시지에 근거하여 보안 관련 변수들을 재설정하고, 기설정된 보안 관련 변수들을 저장하는 단계, 상기 재설정된 변수들을 이용하여 상기 제어 메시지의 보안 검사를 수행하는 단계, 상기 제어 메시지가 상기 보안 검사를 통과하지 못한 경우, 상기 변수들을

복원하는 단계, 상기 복원된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 포함하여 이루어진다.

**【발명의 구성】**

<42> 이하 본 발명의 바람직한 일 실시 예에 따른 구성 및 작용을 첨부된 도면을 참조하여 설명한다.

<43> 도 3은 본 발명의 바람직한 실시예에 따른 보안 설정 제어 메시지의 처리 방법을 나타낸 플로우 챠트이다.

<44> 도 4는 본 발명의 바람직한 실시예에 따른 보안 관련 환경 변수들 중 COUNT-I의 구성을 도시한 것이다.

<45> 도 5는 본 발명의 바람직한 실시예에 따른 무결성 검사의 인증값 생성 알고리즘의 일 예를 도시한 것이다.

<46> 도 3을 참조하면, 먼저 단말기는 수신된 메시지의 타입을 확인한다(S10). 만일, 상기 수신된 메시지가 보안 설정 제어 메시지인 경우, 단말기가 상기 보안 설정 제어 메시지 자체에 대한 보안 검사를 하기 전에, 기설정된 보안관련 환경변수들을 임시로 저장한다.(S11) 그리고, 상기 수신된 보안 설정 제어 메시지에 포함된 보안관련 환경설정정보를 이용하여 보안관련 환경변수를 갱신한다.(S12) 상기 보안 관련 환경변수를 갱신한다는 것은 예를 들어, COUNT-I 값의 상위 28비트 값인 HFN을 다시 설정한다는 것과 같은 것을 의미한다. 이렇게 새로 설정된 HFN은 단말기가 최근에 전송한 START 값, 0, 또는 특정한 값이 될 수 있다. 그리고, 상기 갱신된

보안관련 환경 변수를 이용하여 상기 수신된 보안 설정 제어 메시지에 대한 보안검사를 한다.(S13) 상기 보안 검사 중 무결성 검사를 하기 위해서는 IK(integrity Key), COUNT-I, MESSAGE, Direction (Direction Identifier, 1bit), FRESH와 같은 파라미터들이 필요하다, 상기 IK는 무결성 키(Key)를 나타내는 것으로, RRC 계층의 상위 계층에서 인증 과정을 통해서 생성한 후, RRC 계층에게 알려준다. 이 IK의 값은 무선구간을 통해서 전송되는 값이 아니며, 단말기에서 RRC 계층의 상위 계층과 네트워크(예를 들어, UTRAN)의 RRC 계층의 상위 계층이 서로 특정한 입력 값을 바탕으로 각자 계산해서 사용하는 값이다. 상기 COUNT-I는 무결성 검사를 위한 일련번호에 해당하는 값이며, 도 4와 같은 구조를 가지고 있다. 상기 COUNT-I는 두 개의 영역들로 이루어져 있으며, 일 영역은 28 bit의 RRC HFN(Hyper Frame Number)를 포함한다. 다른 영역은 4bit의 RRC SN(Sequence Number)를 포함한다. 상기 HFN은 전술한 바와 같이, 상기 수신된 보안 설정 제어 메시지에 근거하여 단말기가 마지막으로 UTRAN에 전송한 START 값, 0, 또는 특정값으로 초기화된다. 상기 START 값은 단말기가 UTRAN과의 RRC 계층들간 연결을 시작할 때, SIM 카드로부터 읽어오는 값으로, 상기 UTRAN에 전송된다. 그리고, 상기 단말기의 RRC 계층의 상위 계층으로부터 전송되는 메시지에 포함되어 UTRAN에 전송되기도 한다. 단말기와 UTRAN간에 RRC 계층들간 연결이 이루어지고 있는 상태에서는, 사용중인 COUNT-I값이나 COUNT-C값(암호화에서 사용되는 값이며, COUNT-I와 비슷한 역할을 한다.)의 상위 20bit중 가장 큰 값으로 정의된다. 그리고 단말기와 UTRAN간 RRC 계층들의 연결이 끝날 때에는, 단말기 및 UTRAN의 RRC 계층들에서 사용중인 START 값을 SIM카드에 저장하게

된다. 상기 MESSAGE는 전송되어진 메시지 자체를 의미한다. 상기 Direction는 방향 판별자로서, 상향 (Uplink)인 경우 0, 하향 (Downlink)인 경우 1로 설정한다. 상기 FRESH는 32bit의 값이며, 각 단말기를 위해 존재하며 단말기와 UTRAN간 RRC 계층들의 연결을 시도하는 때에, UTRAN이 상기 FRESH로써 임의의 값을 해당 단말기로 전송한다. 단말기와 UTRAN은 상기 파라미터들의 값을 입력값으로 도 5와 같은 동작을 수행하여 MAC-I와 XMAC-I값을 생성한다. 상기 MAC-I는 UTRAN에서 생성한 무결성 검사 인증값이고, XMAC-I는 단말기에서 생성한 무결성 검사 인증값이다. 따라서, UTRAN/단말기의 모든 입력값들이 같다면 도 5의 과정을 수행하여 생성된 MAC-I값과 XMAC-I값은 같을 것이다. 그런데 중간에 메시지가 변형되었다면, 수신측과 송신측에서의 MESSAGE라는 입력 값이 다르게 되고, 따라서 XMAC-I값과 MAC-I값이 다르게 된다. 따라서, 단말기는 MAC-I값과 XMAC-I값을 비교해서 두 값이 다르다면, 상기 수신된 보안 설정 제어 메시지가 전송 도중 의도적으로 내용이 변경되었거나, 인증되지 않는 곳으로부터 전송되었다고 판단한다. 따라서, 상기 보안 설정 제어 메시지는 유효한 메시지가 아닌 것으로 판단하며, 무결성 검사를 통과하지 못한 것으로 결정한다.

<47> UTRAN은 메시지를 새로 보낼 때마다 도 5의 과정에서 사용되는 입력 값의 일부가 바뀌도록 한다. 그리고 이를 이용하여 매번 새로운 MAC-I가 생성되도록 한다. 이것은 제3자가 MAC-I값을 재사용하여 보안의 허점을 노리는 것을 막기 위해서이다. 이를 위해 UTRAN은 메시지를 새로 보낼 때마다 COUNT-I의 하위 4bit값인 SN값을 1씩 증가시킨다. SN값은 4bit이기 때문에 SN값은 0에서 15까지의 값을

가지게 되고, 0부터 순차적으로 1씩 증가하게 된다. 그리고 SN값이 15가 되면 다음 번 SN값은 0이 되고, 다시 1씩 증가하게 된다. 이렇게 SN이 15에서 다시 0으로 되는 경우마다, COUNT-I값의 상위 값에 해당하는 HFN도 1씩 증가시킨다. 도 4의 COUNT-I의 구조를 보면 명확해 진다. 따라서, 이런 방법을 이용하면 결국 COUNT-I가 매번 1씩 증가하는 것과 같은 효과가 발생하고 위에서 언급했듯 무결성 암호화 인증값 계산 과정의 입력값의 일부가 바뀌게 된다.

<48> 그리고, 단말기는 수신된 메시지의 SN값을 보고 이 값이 한 주기를 돌았다고 판단되는 경우, 자신의 HFN값도 1씩 증가시킨다. 이렇게 해야 송신측과 COUNT-I를 일치시킬 수가 있다.

<49> 이런 방법을 이용하면 SN 정보만 보내더라도 단말기와 UTRAN이 같은 COUNT-I 정보를 가질 수가 있다. 그리고 COUNT-I를 전부 보낼 때 발생할 수 있는 제3자로의 보안정보 누출도 막을 수가 있다.

<50> 따라서, UTRAN은 매번 메시지를 전송할 때마다 수신측이 XMAC-I를 제대로 계산하게 하기 위함과 동시에 보안이 새어나가는 것을 막기 위해서 COUNT-I의 하위 값인 SN값을 메시지에 부가하여 전송한다. 그리고, 단말기가 무결성 검사에서 기준으로 사용할 MAC-I값도 메시지에 부가하여 전송한다.

<51> 그런데 단말기는 이렇게 전송되어온 SN 값이 제대로 된 값임을 검증할 필요가 있다. 이를 위하여 단말기는 지금까지 수신된 SN 값을 이용하여 자신만의 지역변수 SN을 관리한다. 만일, 상기 보안 설정 제어 메시지와 함께 전송되어온 SN 값과 단말기의 지역변수 SN 값이 같다면, 인증되지 않은 제3자가 송신측과 같은 보안

정보를 이용해서 메시지를 보내 왔을 수도 있고, 인증된 UTRAN으로부터 동일한 메시지가 중복되어 전송된 것으로도 볼 수 있기 때문에 단말기는 이 보안 설정 제어 메시지를 즉시 폐기한다.

<52> 단말기는 상기 보안 설정 제어 메시지와 함께 전송되어온 SN값을 이용하여 COUNT-I를 구성하고, 이 COUNT-I와 자신이 기설정하고 있는 파라미터들(메시지, DIRECTION, FRESH)을 이용하여 도 5와 같은 과정을 거쳐서 XMAC-I를 계산한다. 그리고, 상기 단말기는 상기 보안 설정 제어 메시지와 같이 전송되어져 온 MAC-I값과 이 XMAC-I값을 비교하여 수신된 보안 설정 제어 메시지의 무결성 여부를 결정한다.

<53> 상기 수신된 보안 설정 제어 메시지가 무결성 검사를 통과하게 되면, 상기 수신측은 메시지에 포함되어 있던 SN값을 지역변수 SN에 저장하여 다음 번 메시지의 SN값 검사에 이용하도록 한다.

<54> 도 5에서의 f9는 3GPP에서 채택하고 있는 표준화된 무결성 검사 인증값 생성 알고리즘이다.

<55> 상기 FRESH 값은 전술한 바와 같이, UTRAN이 단말기에게 전송하는 임의의 상수값으로, 종래의 COUNT-I값과 MAC-I값을 재사용하는 불순한 단말기로부터 UTRAN을 보호하기 위한 것이다. 만약 FRESH값을 갱신하는 과정이 없다면, 임의의 보안 공격자는 RRC 계층간 연결을 새로이 요구하는 때에, COUNT-I의 상위값으로 쓰일 START 값을 아주 작은 값으로 설정하길 요구하고, 그 이후에는 이전의 RRC 계층간에 연결을 할 때에 사용되었던 SN값과 MAC-I의 쌍을 이용해서 UTRAN의 보안을 무력화시킬 수도 있기 때문이다. 하지만 RRC 계층간 연결이 새로이 만들어질 때마다 UTRAN에서

FRESH 값을 새로 할당하여 이런 보안의 허점을 막을 수가 있게 된다.

<56> 상기 보안 설정 제어 메시지가 보안 검사를 통과하지 못할 경우(S14), 상기 보안 설정 제어 메시지를 폐기함과 동시에 상기 임시로 저장해 놓은 보안 관련 환경 변수들을 복원한다.(S17) 상기 복원된 보안 관련 환경 변수들을 이용하여 이후에 수신되는 메시지를 처리한다. 그러나, 상기 보안 설정 제어 메시지가 보안 검사를 통과한 경우(S14), 상기 임시로 저장해 놓은 보안 관련 환경 변수들을 삭제한다.(S15) 그리고, 상기 수신된 보안 설정 제어 메시지의 잔여 정보에 근거하여 보안 설정 환경 설정 정보를 갱신한다.(S16) 그리고, 상기 갱신된 보안관련 환경 변수들을 이용하여 이후에 수신되는 메시지들의 보안 검사를 수행한다.

<57> 이와 같은 메시지 처리 방법에서, UTRAN으로부터 단말기로 전송되는 도중 내용이 변경되어 전송된 메시지 또는 인증되지 않은 곳으로부터 제공되는 보안설정 제어메시지를 받았더라도 기설정된 보안관련 환경변수의 저장 및 복원과정을 통해서 UTRAN의 보안관련 환경 변수와, 단말기의 보안관련 환경변수를 동일하게 유지시킴으로써 추후 일어나게 되는 메시지의 교환이 불가능하게 되는 상황을 막을 수 있게 한다.

<58> 이렇게 시행된 보안 검사를 통해 수신된 메시지가 유효하지 않다고 판단한 경우, 단말기는 보안설정제어메시지를 폐기하게 되고, 이후의 통신을 계속 유지시키기 위해 저장해 두었던 기설정된 보안관련 환경변수를 다시 복원해서 추후의 메시지에 대한 보안을 유지하게 한다.

<59> 그리고 보안 검사 후, 보안설정 제어메시지가 유효하다고 판단한 경우, 단말

기는 저장해 놓은 기존의 보안관련 환경변수를 폐기한다.

<60> 상기 보안 검사는 전송도중 메시지의 내용이 제3자에 의해 바뀌었다거나 인증되지 않은 곳으로부터 온 것임을 알아낼 수 있는 검사를 의미하며, 무결성 검사 등을 포함한다. 그리고 보안관련 환경변수는 이런 보안 검사를 수행할 때 필요한 HFN값 같은 입력값들을 포함한다.

**【발명의 효과】**

<61> 이상에서와 같이 본 발명은 보안 설정 제어 메시지가 수신된 경우, 기설정된 보안관련 환경변수를 임시저장하고, 상기 보안 설정 제어 메시지의 새로운 보안관련 환경변수를 이용하여 상기 보안 설정 제어 메시지의 무결성 검사를 수행하며, 만약 이 보안 설정 제어 메시지가 무결성 검사를 통과하지 못하는 경우, 상기 임시저장 해놓았던 보안관련 환경변수를 복원하여 네트워크와 단말기의 보안정보 차이로 인한 통신 단절의 문제를 해결하는 효과가 있다.

<62> 이상 설명한 내용을 통해 당업자라면 본 발명의 기술 사상을 일탈하지 아니하는 범위에서 다양한 변경 및 수정이 가능함을 알 수 있을 것이다.

<63> 따라서, 본 발명의 기술적 범위는 실시예에 기재된 내용으로 한정하는 것이 아니라 특허 청구 범위에 의해서 정해져야 한다.

## 【특허청구범위】

【청구항 1】

수신된 메시지가 보안 설정 제어 메시지인 경우, 이 제어 메시지에 근거하여 보안 관련 변수들을 재설정하고, 기설정된 보안 관련 변수들을 저장하는 단계;

상기 재설정된 변수들을 이용하여 상기 제어 메시지가 유효한 메시지인가를 체크하는 단계;

상기 제어 메시지가 유효하지 못한 경우, 상기 저장된 변수들을 복원하는 단계;

상기 복원된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 포함하여 이루어지는 것을 특징으로 하는 이동통신 시스템에서 보안 설정 메시지를 처리하는 방법.

【청구항 2】

제 1 항에 있어서,

상기 제어 메시지가 유효한 메시지인 경우, 상기 재설정된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 이동통신 시스템에서 보안 설정 메시지를 처리하는 방법.

【청구항 3】

제 1 항에 있어서,

상기 메시지의 유효성 체크는 무결성 검사(Integrity Check)에 의해 수행하

는 것을 특징으로 하는 이동통신 시스템에서 보안 설정 메시지를 처리하는 방법.

【청구항 4】

수신된 메시지가 보안 설정 제어 메시지인 경우, 이 제어 메시지에 근거하여 보안 관련 변수들을 재설정하고, 기설정된 보안 관련 변수들을 저장하는 단계;

상기 재설정된 변수들을 이용하여 상기 제어 메시지의 보안 검사를 수행하는 단계;

상기 제어 메시지가 상기 보안 검사를 통과하지 못한 경우, 상기 변수들을 복원하는 단계;

상기 복원된 변수들을 이용하여 이후에 수신되는 메시지를 처리하는 단계를 포함하여 이루어지는 것을 특징으로 하는 이동통신 시스템의 무선 자원 제어 계층에서의 보안 설정 메시지를 처리 방법.

【청구항 5】

제 4 항에 있어서,

상기 보안 검사는 무결성 검사(Integrity Check)를 포함하는 것을 특징으로 하는 이동통신 시스템의 무선 자원 제어 계층에서의 보안 설정 메시지를 처리 방법.

【청구항 6】

제 4 항에 있어서, 상기 보안 관련 변수들의 어느 하나는 상기 보안 검사에 이용되는 COUNT-I 값의 일 영역의 HFN(Hyper Frame Number)을 포함하는 것을 특징으로 하는 이동통신 시스템의 무선 자원 제어 계층에서의 보안 설정 메시지를 처리

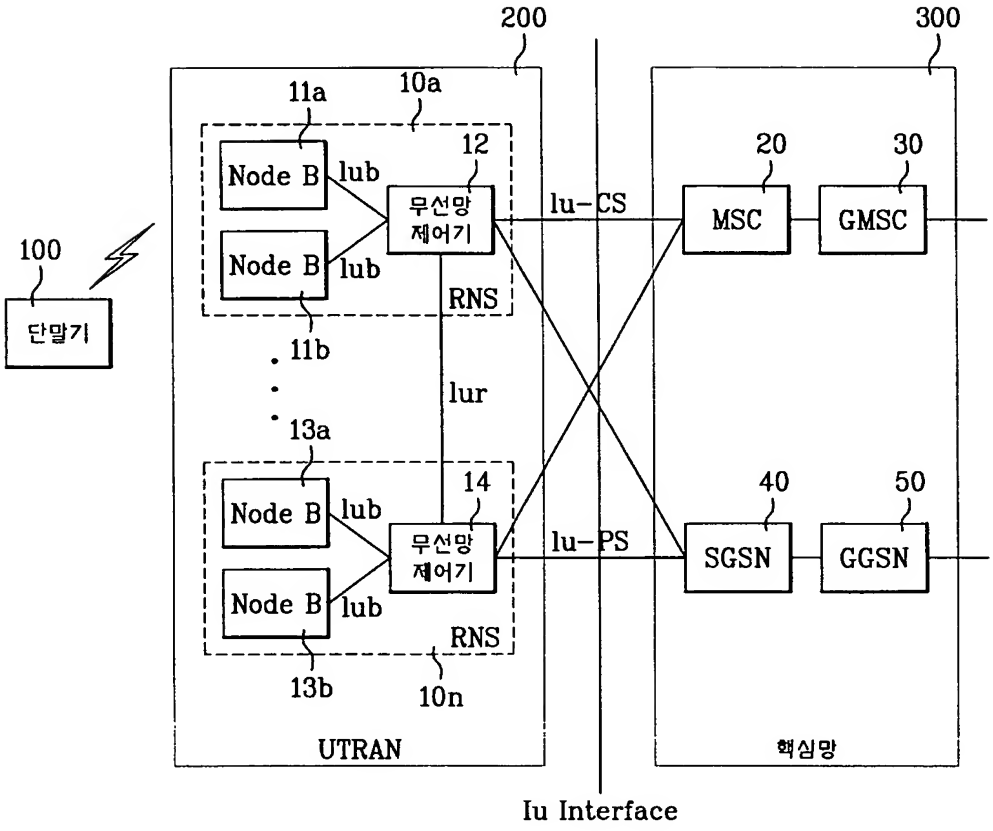
방법.

【청구항 7】

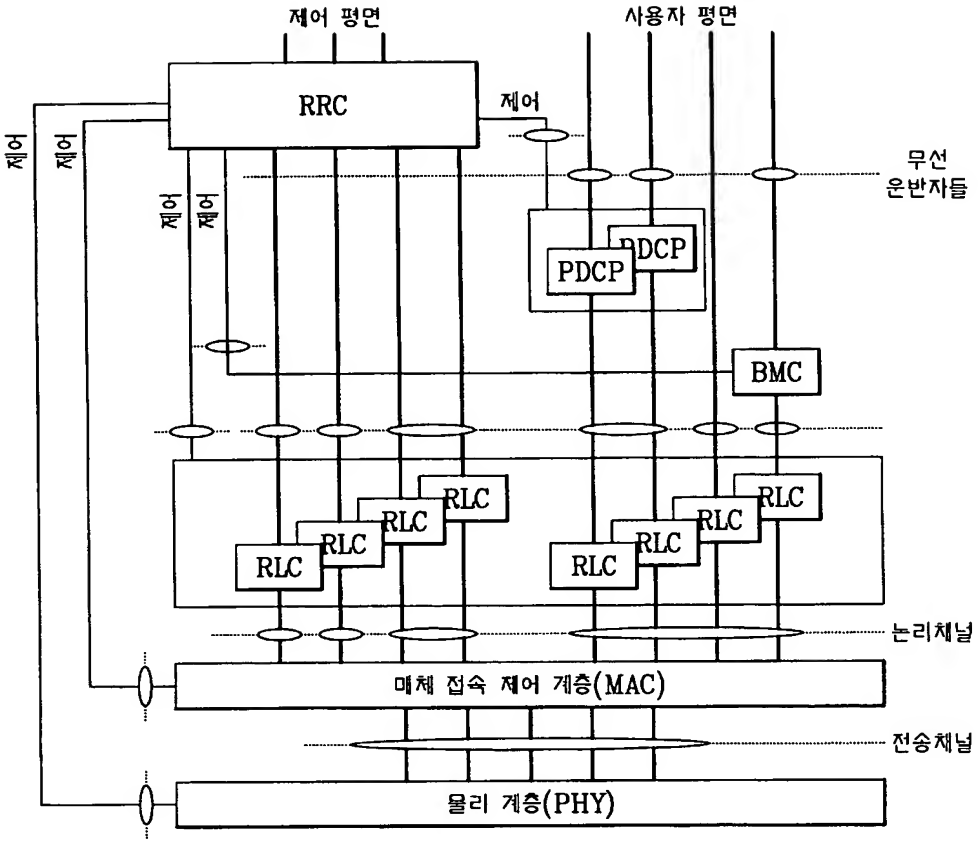
제 4 항에 있어서, 상기 제어 메시지가 상기 보안 검사를 통과한 경우, 상기 저장된 보안 관련 변수들을 삭제하고, 상기 수신한 보안 설정 제어 메시지에 포함된 나머지 정보를 처리하는 것을 특징으로 하는 이동통신 시스템의 무선 자원 제어 계층에서의 보안 설정 메시지를 처리 방법.

【도면】

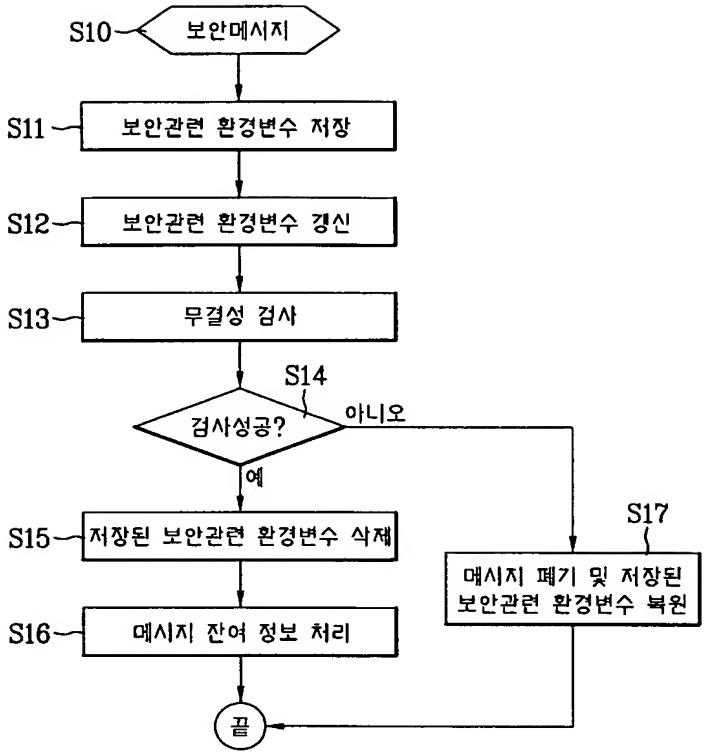
【도 1】


200
300
11a
10a
12
Node B
lub
Node B
lub
무선망 제어기
lu-CS
MSC
GMSC
20
30
100
단말기
RNS
11b
lur
13a
14
Node B
lub
Node B
lub
무선망 제어기
lu-PS
SGSN
GGSN
40
50
RNS
13b
10n
UTRAN
핵심망
Iu Interface

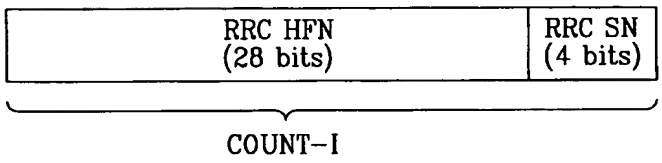
【도 2】


제어 평면
사용자 평면
RRC
제어
제어
제어
제어
무선
운반자들
PDCP
PDCP
BMC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
논리채널
매체 접속 제어 계층(MAC)
전송채널
물리 계층(PHY)

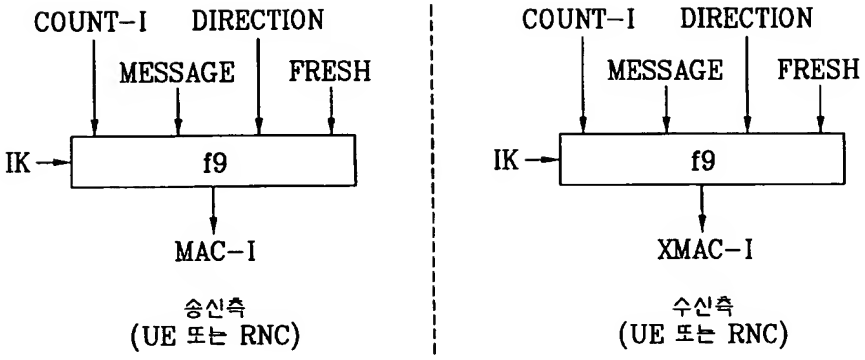
【도 3】


S10
보안메시지
S11
보안관련 환경변수 저장
S12
보안관련 환경변수 갱신
S13
무결성 검사
S14
검사성공?
아니오
예
S15
저장된 보안관련 환경변수 삭제
S16
메시지 잔여 정보 처리
S17
메시지 폐기 및 저장된
보안관련 환경변수 복원
끝

【도 4】


RRC HFN
(28 bits)
RRC SN
(4 bits)
COUNT-I

【도 5】


COUNT-I
DIRECTION
MESSAGE
FRESH
IK
f9
MAC-I
송신측
(UE 또는 RNC)
COUNT-I
DIRECTION
MESSAGE
FRESH
IK
f9
XMAC-I
수신측
(UE 또는 RNC)